Initial Call For Papers

Journal of Sensitive Cyber Research and Engineering (JSCoRE)

Science advances best when it includes peer review and dissemination of materials. Until now, potential authors conducting non-public cybersecurity research have had no widely-recognized, high-quality and secure venue to publish their results. The U.S. government sponsored Journal of Sensitive Cyber Research and Engineering (JSCoRE)[1] will balance both the need to protect sensitive information, and the need to support scientific information exchange. JSCoRE is the first of its kind peer-reviewed journal for high quality, non-public cybersecurity research, advanced engineering results, and case studies. JSCoRE provides authors in government, industry and academia with the opportunity to receive cross-organization visibility and input. JSCoRE is intended to foster collaboration among researchers, increase the availability of results to those seeking to enhance cybersecurity operations, provide peer review to validate research activities, and facilitate recognition of the author(s) contribution to advancing the state-of-art for cybersecurity.

We seek previously unpublished, high-quality papers describing non-public research in the field of cybersecurity that advances the state-of-the-art or provides significant insights for application of existing or new technical capabilities toward achieving effective cybersecurity operations. The Journal will consider the following in deciding whether to accept a submission for publication:

- The submission must be appropriately portion marked by the submitting organization;
- The submission must meet the key publication requirements of high quality research and broadly useful information whether describing successes to build upon or failures to learn from and avoid;
- The submission may relay (i) conceptual ideas for guiding further research or achieving effective operations, (ii) review of existing research to evaluate, systematize, or contextualize existing knowledge, (iii) a work in progress, or (iv) a completed work;
- The submission must be inherently non-public at time of submission, that is, an integral aspect of the work must be either (i) controlled unclassified information (e.g., export controlled, Official Use Only, For Official Use Only, Sensitive But Unclassified, etc.) or (ii) classified information (that is, collateral Confidential up to Top Secret//SI/TK//NOFORN);
- The submission must be releasable to all members of the cybersecurity community with the appropriate clearance and formal access approvals, for example, the Journal will not accept a paper with originator-controlled distribution; and
- The submission should include (perhaps in addition to sensitive versions) a publicly-releasable title, abstract, and citation whenever feasible to facilitate public indexing of Journal contents.

[1] The Journal of Sensitive Cyber Research and Engineering (JSCoRE) is an initiative of the Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group which coordinates research activities related to national security systems.

Topics of Interest: Being the only repository for non-public, peer-reviewed, journal-quality research, the Journal actively seeks papers across the full range of topics related to cybersecurity. For the Journal 'cybersecurity' encompasses all aspects of cybersecurity research and engineering; recognizing and encouraging adversarial perspectives in published works. Additionally, in recognition of the multi-dimensional nature of the cybersecurity problem, the Journal seeks input from a wide range of disciplines, sectors, sciences and technologies – drawing on expertise not only from mathematics, computer science, and electrical engineering, but also biology, economics, and other social and behavioral sciences as they specifically relate to cybersecurity. Papers whose sole advancement is in crypto-science or crypto-mathematics are explicitly excluded.

Certifications: Author, security classification, and release approval certifications must be provided as separate documents, either with electronic signature or as scanned versions of physically signed documents. Certification templates detailing the necessary verifications can be obtained through the additional information email address at the end of this call for papers.

Copyright: The author is responsible for obtaining approval to use any copyrighted material contained or referenced in the paper. The Journal will provide guidance on 'fair use' if necessary. Papers written by government employees for government publication are not copyrighted. Papers written by non-government employees are copyrighted and the copyright belongs to the author or the author's organization, depending upon the contractual relationship between the author and his/her organization.

Formatting:

In this initial call, papers are to be formatted for 8.5x11 inches including all figures and graphics, less than 20 pages long (striving for concise expression that fully addresses the subject), written in English, and compliant with the following formatting:

Times New Roman, 12-point font, single-spaced, one-inch margins;

References use end notes in brackets (no footnotes);

Left-justified heading placement for sub-titles and sections;

Author line contains all authors, with one designated as the corresponding author with contact information;

Paper includes a one or two paragraph abstract summarizing the work and its significance to the cybersecurity community and typically the following sections: Introduction, Related-Work, [body of paper with titles and sectioning as deemed appropriate], Conclusion (and Recommendations), Acronyms/Glossary (if necessary), References, and Acknowledgements;

Tables and figures should be embedded and captioned independently so as to allow full text searches;

Acknowledgements should include (as applicable) funding source, technical support, and other research support;

All papers must contain classification markings per U.S. National Archives, Information Security Oversight Office (ISOO) instruction (http://www.archives.gov/isoo/training/marking-booklet.pdf).

Publishing Venue: The first edition of the Journal will be initially published as a separate sub-topic under the existing Journal of Intelligence Community Research and Development (JICRD) on the Joint Worldwide Intelligence Communications System (JWICS) network. Future publications will allow for access at lower classification levels, and may include optional indexing where appropriate.

Submission: The Journal is a web-based publication with no fixed submission date other than papers submitted with certifications by 31 January 2013 will be considered for publication in the first edition of the journal in April 2013. Papers submitted after 31 January 2013 will be considered for publication at a later date. Papers should be submitted electronically with Microsoft Word® .doc or .docx being the preferred file format and editable PDF also being acceptable. Certifications should be submitted electronically in PDF format.

For more information: For more information; to include the latest version of the Journal Call for Papers, instructions for submission, and copies of certification templates; go to http://cybersecurity.nitrd.gov/jscore or email jscore@nitrd.gov. Those wishing to participate as reviewers or join our potential author mailing list are encouraged to submit their names and contact information to jscore@nitrd.gov and the journal editorial staff will provide further information.